Annex D
Copy 4

~~TOP SECRET~~

TICOM/I-175

REPORT BY ALFRED POKORN, OF OKH/CHI, ON M.209

Attached is a report on the M.209 written at our request in English by ALFRED POKORN of OKH/Chi.

The report was written at VIENNA during November, 1945, and was received from G.S.I.(S), B.T.A. through M.I.8.

TICOM

14th December, 1945

No. of Pages: 12

Distribution:

British

D.D.3
H.C.G.
D.D.(M.W.)
D.D.(A.S.)
C.C.R.
Cdr. Tandy
Major Morgan

U.S.

Op-20-G (4) (via Lt. Cdr. Manson)
G-2 (via Lt. Col. Hilles)
A.S.A. (4) (via Capt. Collins)
Director, S.I.D. USFET
Col. Kunkel, USAAFE

TICOM

S.A.C. (3)
Cdr. Bacon
Lt. Cdr. Manson
Major Cowan
Capt. Collins
Ticom Files (4)

The Convertor M 209.

A ciphering and deciphering machine of the type "Haegelin", manufactured in SWEDEN. Worked by hand or by electricity. Essential parts:

6 wheels, with 17, 19,21,23,25 and 26 pins, all of them corresponding to letters of the alphabet showing on the wheels. The pins can be set to be active or inactive.

1 drum with 27 bars, bearing 1 or 2 lugs each. These can be set to be active or inactive. If at least 1 lug is active, the bar can be made to protrude sideways from the drum. The lugs are set in rows corresponding to the wheels and so as to be touched by the active pins, when the drum is turned.

1 printing wheel, with 2 sets of the letters of the alphabet, arranged in alphabetic but opposite order, one for clear writing, the other for cipher writing:

Clear: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Ciph: Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

When ciphering, the clear letter wanted is ~~printed~~ first. Then the wheels are turned by one pin position each, and the drum is turned once round. This makes the active pins work on the lugs set before them - if there are any - and so pull sideways a number of bars. At the same time, these bar work on teeth fixed to the printing wheel, turning that wheel round by so many letters as there are bars protruding from the drum. This turn can cover from 0 to 25 letter-spaces on the printing wheel. 26 bars protruding equal 0 bar, 27 bars equal 1 bar in effect. Then only the cipher letter is printed.

When deciphering, the cipher letter is printed first and the movements as above result in a turn of the printing wheel that will print the corresponding clear letter.

The converter supplies a substitution-cipher, with alphabets changing from letter to letter, according to the turns of the printing wheel between clear and cipher. There are but 26 substitution alphabets, but the order of their following one another depends on the setting of the pins and lugs, and that can be varied practically without limits. With a given setting of pins and lugs, the order of substitution alphabets will be repeated after 17 x 19 x 21 x 23 x 25 x 26 = about 105 million letters printed.

The Ciphering System

The U.S.A. used the converter for messages of minor importance between units of various signal nets. For every net, key lists were issued, giving the setting of pins and lugs - internal indicator - for one month, or for periods fixed as "D-Day", "D-day + 1", "D-day + 2" etc. The setting changed from day to day.

The system was used in AFRICA, SICILY and ITALY, as well as in FRANCE and on the Western front.

Messages were sent in 5-letter groups. The first and the last two groups of every msg. - external indicator - were identical. Of these, the first two letters, always identical, were the key for changing the wheels from the initial position to starting position. The next 6 letters were the initial position of the wheels. The last two letters indicated the signal net and the key list used for the internal setting.

When ciphering, the pins and lugs had to be set according to key list and date - internal setting -, the wheels were turned to any chance position - external setting - and the letters then showing on the wheels were used for the 3rd to 8th letter of the external indicator of the message to be sent. Then any letter of the alphabet was printed several times, this clear letter being used as the first 2 letters of the external indicator. The first letters of the cipher text produced by this printing, were then turned on on the wheels. As only one of the wheels bears all the letters of the alphabet, usually more than 6 letters had to be printed to provide letters suitable for all the wheels. After that, the ciphering could begin. Words were spaced by printing clear "Z".

When deciphering, the pins and lugs had to be set as above. The wheels were turned to the initial position given by the 3rd to 8th letter of the external indicator. The letter 1st and 2nd of the indicator was printed several times. The wheels were turned to the letters resulting of this printing and the deciphering of the message could begin. Cipher letters corresponding to clear "Z" left the word-to-word spaces in the clear text.

The Breaking of the Cipher

The Cipher can be broken in four cases only:

1. When there are two different messages available, ciphered by one signal net, on the same day, and with an identical starting position of all wheels - same external indicator - so that internal and external settings are identical.

   This may be subsequent messages of one station, or a message and the answer thereon, the operator of the 2nd message or the answer turning back the converter to the starting position of the 1st message and neglecting to change the external setting, for the 2nd message or the answer.

2. When there are two identical messages available, ciphered by one signal net, on the same day, and with an identical starting position of 4 or 5 wheels only, but with the same external indicator, so that internal settings are identical and external settings differ slightly.

   This results by an error in the setting of the wheels to starting position, the typing of the single letter producing e.g. RSQTRFJ and the operator turning the wheels to RSORFJ, in the 1st message. The 2nd message is a correct repetition of the 1st, with identical external indicator.

3. When there are two identical messages available, ciphered by one signal net, on the same day, and with an identical initial position of the wheels, but with a starting position deplaced by one or two letters (or pins) equally on all wheels.

This results by printing another single letter, than the two first letters of the external indicator, for changing the initial wheel position to the starting position, in the 1st message. The 2nd message is a correct repetition of the 1st, with identical external indicator. If the correct single letter differs from that used for ciphering message I, by one letter of the alphabet (e.g. M and N), the starting position of both messages will also differ by one letter - or pin position on all wheels. Same for two (and more) letters, so long as no letters are printed, that could not be turned on on the respective wheel.

4. When an original key-list is captured.

Identical internal and external settings.

For the following the cipher texts of the two messages be supposed as:

Message I: Z C L N H . . . . .
Message II: N H I O O . . . . .

Both first letters were printed with the identical converter settings and with the same turn of the printing wheel from clear to cipher. Thus, assuming certain clear letters for the 1st cipher letter in Message I, it can be told what the first clear letter in Message II must be.

The apparatus for this is a working model of the printing wheel, two tapes with alphabets written in opposite direction:

. . . . . M N O P Q R S T U V W X Y Z

Z Y X W V U T S R Q P O . . . . . .

If in message I clear A stands for cipher Z, the tapes arranged so that A and Z correspond, show that N and M correspond, and that in message II clear M stands for cipher N.

Assuming all the alphabet in turn, that would show as the 1st clear letters:

Message I:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Message II:	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L

If cipher C is clear A, then cipher H is clear V. If L is A, then I is D. If N is A, then O is Z. If H is A, then O is T. That would show the first five clear letters to be:

Message I:	(1st to 5th letter):	A B C D E F G H I J K L M N O . . .
Message II:	(1st letter):	M N O P Q R S T U V W X Y Z A . . .
	(2nd "):	V W X Y Z A B C D E F G H I J . . .
	(3rd "):	D E F G H I J K L M N O P Q R . . .
	(4th "):	Z A B C D E F G H I J K L M N . . .
	(5th "):	T U V W X Y Z A B C D E F G . . . .

If for any part of Message I the correct clear text can be guessed, the corresponding part of Message II shows clear text also, though the text is different from that in Message I. Assuming in the example above, the first word in Message I to be "ONE", the first word in Message II must be "AIH", so "ONE" at this place is wrong.

It is necessary to try "mots probables " until the correct word is found. For that, the table as above is cut in vertical stripes, and words are set with the letters of Message I in ascending order, so that the corresponding text of Message II may be read horizontally. Example for a break:

Z	O	N	E	Z
L	A	Z	Q	L
U	J	I	Z	U
C	R	Q	H	C
Y	N	M	D	Y
S	H	G	X	S
	I	S	K	Z
		X	P	L
			Z	G
			O	

The 5th to 9th letter in Message I spell "-ONE-" in Message II: "SIX-O", possibly "SIX-ONE-".

The break is extended to both sides, either by continuing work with the vertical stripes, or by using the model of the printing wheel only. A break of 60 to 100 clear letters is sufficient for further work.

Examples for "mots probables":

Numbers, signs (dash,paren,cma,etc), short words (at, in,to,etc), endings (-ing,ation,etc.).

With all the above, one can read the original two messages only, as far as broken. Before deciphering or reproducing the ciphering of these messages on the converter, the internal setting of the latter has to be found.

Idnntical internal and slightly different external settings.

The cipher texts of the two messages are partly identical, partly different. Were they differ, there is at least one pin positiom wrong. From the space from correct letter (Message II) to wrong letter (Message I) it is possible to deduce the action of the wheel that was in the wrong starting position.

Details are unknown to me. Messages with three or more wheels set in a wrong starting position cannot be broken.

Deplaced starting position.

If the starting positions of the wheels for two messages ciphered otherwise under identical conditions, are displaced by one (letter or pin) equally on every wheel, the sequel of turns of the printing wheel is in both messages identical, but displaced by one (letter-space). By writing the messages displaced by one letter, the cipher letters resulting from the same turns of the printing wheel are above one another: E.g.

Message I : W G Q B P . . . . . .
Message II : F S I P P J . . . . . .

Supposing W(Message I) is A, then S (Message II) is E, as the model of the printing wheel shows. S is 2nd letter of the text, so cipher G (Message I) must be clear E too.

If G is E, then I is C. That is the 3rd letter of the text, so Q (Message I) must be C too. If this is so, P is D, and B as 4th letter is the same. If B is D, then the P underneath is P, etc. So if the initial W is clear A, the clear text of the messages should read:

A E C D P

which is wrong. By assuming all letters of the alphabet in turn, for the first cipher letter, however, the correct clear text must be found:

A E C D P V . . .
B F D E Q W . . .
C G E F R X . . .
D H F G S Y . . .
E I G H T Z . . .

The messages begin both "EIGHT" and this can be extended easily, by the same method.

If two messages are displaced by two or more positions, they must be written down displaced accordingly, and then worked on as messages with identical internal and external indicators.

Finding The Relative Internal Setting.

This consists in setting, on every wheel, the pins in the correct sequel of active or inactive positions, but without beginning the sequel at the correct spot of the circumference of the wheel. E.g.

Letters on the wheel: A B C D E F G H I J K . . .
Absolute correct sequence: + + - + - - - + - + + . . .
Relative correct sequence:
(displaced by two): - + + + - + - - - + - . . .

There is but one way of setting the lugs on the drum bars. This, and the setting of the pins, makes the internal setting of the converter.

The clear text of a broken message and the cipher text of the same, are written one under the other, to show over how many letter-spaces the printing wheel turned before printing every cipher letter. As Z and A are, on the printing wheel, side by side, clear A would result in cipher Z by the space 0, in cipher A by the space 1, in cipher B by the space 2, etc.

Clear B would result in cypher Y by the space 0, in cypher Z by the space 1, in cypher A by the space 2, etc. E.g.

Clear:	R	E	Z	Y	O	U	R
Cipher:	E	V	F	D	C	P	S
Spaces:	23		5	17		10	
		0		2	10		

This gives a sequel of spaces in the length of the broken message.

The sequel is written in six tables, with 17,19, 21,23,25 and 26 numbers respectively, written in one line. Every table indicates the wheel corresponding to the breadth of the case. E.g.

Wheel 17:	23	0	5	2	17	10	10	21	8	20	11	15	7	12	25	0	5
	25	6	2	3	22	8	9	20	2	25	5	25	3	17	21	9	6
	20	9	8	0	25	4	4										

The spaces showing in one column (one under the other) have been produced with the wheel being in a certain position, identical for all the spaces in that column. From the spaces in a column being large or small, it can be said whether the pin in that position of the wheel must have been active or inactive. Active pins have contributed to make the space large. Small spaces in one column show that the wheel must have been inactive in that position. The sequel of pin positions for the wheel above would be:

+ - - - + - - + - + - + - ? + - -

By comparing the different wheels, sequels of pin positions, though incomplete, can be made up for most of the wheels.

By continued comparing and correcting the sequels, they can be made complete. By comparing them with the turns made by the printing wheel to produce every cipher letter, moreover, the working of the drum bars, and the positions of the lugs on them, can be deduced.

The result is the complete, though relative, internal setting of the converter. Before deciphering of other messages with the converter is possible, though these messages be ciphered with the same internal settings, the absolute internal setting has to be found.

The Absolute Internal Setting

As has been said before, the position of the active and inactive pins on every wheel, relative to the letters on the wheel, must be found. The sequel of the pin positions of every wheel is known, and so are the positions of the drum bar lugs.

The sequel of spaces covered by the turns of the printing wheel, from the beginning of the message text, is known. It is found by comparing the clear and the cipher text of the message and using the model of the printing wheel. E.g.

Clear:	R	E	Z	Y	O	U	R	Z	M	S	G	.	.	.
Cipher:	E	M	A	P	O	T	S	S	C	B	W	.	.	.
Spaces:	22	17	0	14	3	14	10	18	15	20	3	.	.	.

Every space is the result from 1 to 5 possible combinations of active or inactive pin positions on the 6 wheels. When the sequel of spaces is long enough, certain sequels of pin positions can be made out. E.g.

		(§)									
Wheel	I:	+	+	−	+	−	−	−	+	+	+ etc.
"	II:	+	−	−	+	+	+	+	+	−	− etc.
"	III:	−	−	+	+	−	−	+	+	−	− etc.
"	IV:	−	+	−	+	−	+	+	+	−	− etc.
"	V:	−	−	−	+	+	+	−	−	−	+ etc.
"	VI:	+	+	−	+	−	−	+	+	+	+ etc.

The vertical columns of this table correspond to the 1st, 2nd, 3rd, etc. letter of the message text. The column (§) as corresponding to the first, indicates the pin positions at the letters on every wheel, that move, when the message text begins to be printed. These are the letters referred to as starting position of the wheels.

The idea about the absolute internal setting, is to begin the arrangement or sequel of pin positions (column §) at such letters of the wheels, that when the wheels are turned to initial positions - external indicator - and the single letter of the alphabet is printed, the 1st printing of this letter will give as cipher the letter, where om wheel I the sequel of pin positions begins; the 2nd printing of the single will give as cipher the letter, where on wheel II the sequel of pin positions begins, etc.

E.g. External indicator: FFCOH BDEQR.
The wheels are turned to the positions

Wheel	I:	C
"	II:	O
"	III:	H
"	IV:	B
"	V:	D
"	VI:	E

and the letter F is printed repeatedly, with results as follows:

1st printing: Clear F, by 1st space of the printing wheel, gives cipher ♀ (wheel I)
2nd printing: Clear F, by 2nd space, gives cipher ♂ (wheel II)
3rd printing: Clear F, by 3rd space, gives cipher ♂ (wheel III)
4th printing: Clear F, by 4th space, gives cipher ♂ (wheel IV)
5th printing: Clear F, by 5th space, gives cipher ♂ (wheel V)
6th printing: Clear F, by 6th space, gives cipher ♀ (wheel VI).

The six spaces or turns of the printing wheel can be drawn as a table, e.g.

Spaces:	1	2	3	4	5	6
Wheel I:	+	+	-	-	+	-
Wheel II:	+	-	+	-	-	-
Wheel III:	-	-	+	+	-	-
Wheel IV:	+	+	+	+	-	-
Wheel V:	-	+	+	-	-	+
Wheel VI:	-	-	-	+	+	+

If the table is right, the columns (vertical) must be possible combinations of pin positions, but also the lines must be possible sequels of pin positions on the respective wheels, and the letters resulting by the printing of clear F and the space in question must be such as exist on the respective wheel.

This must be tried and varied so long as to get a table responding to this conditions.

When the table is found, the cipher letters resulting by the printing of "FFFFFF ..." and the spaces shown in the table, give the starting position of the wheels. At these, the sequels of pin positions have to begin (♀ on page 8).

If the absolute internal setting cannot be found this way - as often it cannot - a third message with the same internal setting (of the same day and signal net) has to be broken first.

Breaking A Third Message.

The relative internal settings of this message are known by having broken two messages of the same day and signal net, and fixed their relative internal settings. This message, however, cannot be deciphered on the converter (as no message other than the two broken messages can) before the absolute internal settings are found out.

The relative internal setting being given, it can be said, for every turn of the printing wheel, which of the 6 wheels took by means of pins an active, or an inactive, part at it. So a list of turns, or spaces, is made up. E.g.

Space:	0	1	2	3	4	etc.
Wheel I	- -	+ +	-	+	-	
Wheel II	- +	- +	+	+	-	
Wheel III	- +	- +	-	-	+	etc.
Wheel IV	- +	- +	-	-	-	
Wheel V	- +	- +	-	-	-	
Wheel VI	- +	- +	-	-	-	

There are, for every letter printed, $2^6 = 64$ possible arrangements of + or - pin positions on the 6 wheels. So several of the 25 possible spaces produced by the printing wheel, can be produced by more than one arrangement.

The sequel of + and - pin positions on every wheel is also known.

A "mot probable" is now tried at the beginning of the message. The spaces that must have been made, if the supposition is correct, are derived from the given cipher, and the possible clear, text. A table with the possible spaces and pin positions is drawn accordingly. E.g.

Cipher text:	J	E	M	Q	E	H	G
Clear text:	Z	E	I	G	H	T	Z
Spaces:	9	9	21	23	12	1	6
Wheel I	+	+	+	+	-	+	-
" II	+	+	+	+	+	-	-
" III	-	-	+	+	-	-	+
" IV	-	-	-	+	-	-	-
" V	+	+	-	+	+	+	-
" VI	-	-	+	-	-	-	-

When more than one pin position arrangement is possible for a space, so many tables have to be drawn, as are possible.

Then the horizontal lines are compared with the sequels of pin positions for every wheel. If they are possible, i.e. if they are sections of these sequels, the table is correct, and the supposed word really stands in this part of the clear text.

The sequels of pin positions are then completed sideways (or to both sides) through the whole of the message. From the vertical columns the spaces are derived. The cypher letters and the spaces belonging to them give the clear letters. The message can be read throughout.

If the horizontal lines in the table are <u>not</u> part of the sequels of pin positions on the wheels, the table is wrong and the supposed word is not there. Then the "mot probable" has to be tried in the same way right through the message.

If one "mot probable" has been tried throughout without success, others have to be tried, until the table of + and - is correct.

With a third broken message at hand, the method of finding the absolute internal setting of the day and signal net, is the same, as described above. Work, however, is greatly reduced in length, by combination of the conditions set to the table to be drawn, from the first two, and the third, message. Many possible cases can be eliminated quickly and the overlooking of the correct table is not so easy, as when working on two messages only.

With the absolute internal setting found, and used on the converter, all available messages of the day and signal net, can be deciphered.

Deciphering With The Converter.

Messages that had a good transmission and reception, i.e. where the cipher text at hand is correct, are deciphered without difficulty, as explained above (page 3). Frequent difficulties are:

1) Ciphering mistakes. They have been dealt with above.

2) Transmission mistakes: Letters or groups of letters have been left out or inserted, or both. To decipher such messages, letters or groups of letters have to be inserted or left out.

3) Reception mistakes. The operator did not get the correct Morse letters. Frequent mistakes are e.g.

B - D, E - I, G - M, H - I, S - H, U - V, Z - G.

Captured Key Lists.

During temporary U.S. retreats in NORTH AFRICA and ITALY, some times original converters and key-lists were captured. Containing the original internal settings for one net and one month, they served to decipher all messages available of this signal net and this period.

One key-list used on D-Day and a few days afterwards, was captured after the invasion in FRANCE had begun.

In every case, the period covered by key-lists captured was over, when they came in German possession. So it was never possible to read current signalling with them, even if the keys were not altered, when the loss of the key-lists was ascertained, as was to be expected.

Working Results.

Messages were broken in a time ranging from 2 hours to 4 weeks. Many of them were not broken at all, owing to the difficulty of guessing a word of the clear text, or to too many transmission, or reception, mistakes.

The finding of the relative internal settings took about 1 day, that of the absolute internal settings from 1 day to 4 weeks. The breaking of a third message also often took 2 to 4 weeks.

With an absolute internal setting found, from 2 to 50 messages of the same day and signal net were deciphered.

From the messages come in, about 10 percent went deciphered.

What Messages Were About.

The following groups of messages and samples of clear text can be remembered:

Supplies: Laundry open at once near cross-road 832045.
Secure large envelope from under Novaks jeep seat.
Send ten tonner for ammo. to .....

Tactical: C.P. at 830716.
Headache red advancing N.E., no resistance.
Réchicourt occupied at 1400 hours., 744018.

Air Support: Bomb line bridge 273406, then railway to ...
Your demand accepted. Aspo.
GRAZ bombed by instruments.

Personal: Send pass for Sgt.White to go to PARIS to-morrow.
Lt. Black is to report to this HQ to be promoted.
Report 2 o., 4nco., 290 em.

Signalling: Traffic report, out 10 secret, 20 confidential,
150 ordinary messages, in 12 secret, 16 confidential,
125 ordinary messages.

Names and numbers of units were given, but cannot be remembered, except such as HEADACHE, FOOTBALL, EGG-CUP etc.

Names of officers cannot be remembered, except Major Longino, aspo, from the FRANCE front.